HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200207237-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Christoph GOUGUENHEIM et al.	Confirmation No.:	2133
Application No.:	10/733,434	Examiner:	Izunna OKEKE
Filing Date:	December 10, 2003	Group Art Unit:	2432

Title: TRUSTED SYSTEM FOR FILE DISTRIBUTION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on December 17, 2009 .

☒ The fee for filing this Appeal Brief is $540.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $130	☐ 2nd Month $490	☐ 3rd Month $1110	☐ 4th Month $1730

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 540 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Christoph GOUGUENHEIM et al.

By: /Ashok K. Mannava/

Ashok K. Mannava

Attorney/Agent for Applicant(s)

Reg No. : 45,301

Date : December 21, 2009

Telephone : (703) 652-3822

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Christoph GOUGUENHEIM et al.	**Confirmation No.:**	2133
Serial No.:	10/733,434	**Examiner:**	Izunna OKEKE
Filed:	December 10, 2003	**Group Art Unit:**	2432
Title:	TRUSTED SYSTEM FOR FILE DISTRIBUTION		

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action dated September 17, 2009 and in connection with the Notice of Appeal filed December 17, 2009.

It is respectfully submitted that the present application has been at least twice rejected.

Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

TABLE OF CONTENTS

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1-7, 9-24, 26-28 and 30-36 are pending and stand rejected.

Claim 8, 25 and 29 are canceled.

Pursuant to 37 C.F.R. § 41.37, the Appellant hereby appeals the Examiner's decision finally rejecting all of the pending claims to the Board of Patent Appeals and Interferences. Therefore, claims 1-7, 9-24, 26-28 and 30-36 of this application are appealed.

(4) Status of Amendments

No amendment was filed subsequent to the Office Action dated September 17, 2009.

A copy of the claims at issue on appeal is attached as the Claims Appendix.

(5) Summary of Claimed Subject Matter

Claims 1, 11, 17, 19, 26, 28 and 36 are the independent claims in this appeal. It should be understood that the subject matter of the independent claims recited below is supported in at

least the following cited sections of the present application. Thus, other sections in the present application may provide the same or additional supports as well.

Claim 1. A secure token (216 in Fig. 2; paragraphs 22 and 25) for use with an encrypted file and an insecure decryption device (212 in Fig. 2), the secure token comprising a processor for protecting a first cryptographic key (K1; paragraph 30) against unauthorized access, and creating a second cryptographic key (K2; paragraph 32) from the first key and a message unique to the insecure device (N; paragraph 27), the second key usable for file decryption by the insecure device, wherein, in a file transaction with a peer, the secure token is configured to create a third key ($K_{2,2}$; paragraph 40) unique to the peer and send the third key to the insecure device and the peer (Steps 520 and 522 in Fig. 5; paragraphs 40-41).

Claim 11. An article for a secure device (216 in Fig. 2; paragraphs 22 and 25), the secure device including a processor, the secure device used in combination with an insecure device (212 in Fig. 2), the article comprising memory encoded with data for instructing the processor to protect a first cryptographic key (K1; paragraph 30) against unauthorized access, use a hash function to create a second cryptographic key (K2; paragraph 32) from the first key and a message unique to the insecure device (N; paragraph 27), and send the second key to the insecure device (paragraph 35; Fig 4), wherein, in a file transaction with a peer, the processor is configured to create a third key ($K_{2,2}$; paragraph 40) unique to the peer and send the third key to the insecure device and the peer (Steps 520 and 522 in Fig. 5; paragraphs 40-41).

Claim 17. A data rights management server (110 in Fig. 1; Fig. 3) for use with a media transaction system (Fig. 1), the server comprising a processing unit programmed to cause the server to establish a secure channel with a smart card (214 in Fig. 2; paragraphs 22 and 25), access a unique identifier (N; paragraph 27) corresponding to an insecure device (212 in Fig. 2), send a first cryptographic key (K1; paragraph 30) to the smart card via the secure channel, receive a unique identifier from the insecure device, create a second key (K2) from the first key and the identifier, encrypt a media file with the second key, and send the encrypted media file to the insecure device, the first key corresponding to the media file (Fig. 3; paragraphs 32-34), wherein, in a transaction with a peer for the media file, the smart card is configured to create a third key ($K_{2,2}$; paragraph 40) unique to the peer and send the third key to the insecure device and the peer (Steps 520 and 522 in Fig. 5; paragraphs 40-41).

Claim 19. A method (Fig. 7) of using an insecure decryption device for file distribution, the method comprising:

accessing a message unique to the insecure device (N; paragraphs 27 and 60-61; 710 in Fig. 7);

accessing a first cryptographic key (K1; paragraphs 60-61);

creating a second cryptographic key from the message and the first key; (K2; paragraphs 63-64; 712 in Fig. 7)

allowing the insecure device to access the second key but not the first key; whereby the insecure device can use the second key for decryption; (paragraph 65, fig 7)

in a file transaction with a peer, creating a third key ($K_{2,2}$) that is unique to the peer; and

in the file transaction, sending the third key to the insecure device and the peer (Steps 520 and 522 in Fig. 5; paragraphs 40-41).

Claim 26. An insecure device (212 in Fig. 2) for use with a secure device (214) and a first cryptographic key (K1), the device comprising:

means for sending a message to the secure device, the message being unique to the insecure device; (paragraphs 60-61, fig 7 and paragraph 27, figs 3-4)

means for receiving a second cryptographic key (K2) from the secure device, the second cryptographic key being derived from the message and the first cryptographic key; (paragraphs 65-66, fig 7 and paragraph 32-34, figs 3-4)

means for performing decryption on a media file with the second cryptographic key; (paragraph 66, fig 7 and paragraph 35, figs 3-4)

means for receiving a third cryptographic key ($K_{2,2}$) derived from a message unique to a peer device, wherein the third cryptographic key is received by the peer device and used by the peer device for decryption (paragraphs 40-41); and

means for encrypting the decrypted media file with the third cryptographic key (paragraph 42).

Claim 28. A trusted system (210 of Fig. 2; Fig. 6) for file distribution, the system comprising:

an insecure device (212 in Fig. 2; 614 in Fig. 6); and

a trusted secure device (214 in Fig. 2; 612 in Fig. 6) for storing a first cryptographic key (K1; paragraph 59), accessing a message from the insecure device (N; paragraphs 61-62) wherein the message is unique to the insecure device, creating a second cryptographic key (K2) from the message and the first key (712 in Fig. 7; paragraph 63), and allowing the insecure device to access the second key, the first key granting file access rights (paragraphs 64-69);

the insecure device not allowed to access the first key, the insecure device using the second key for decryption (paragraphs 64-69), wherein, in a file transaction with a peer, the trusted secure device is configured to create a third key ($K_{2,2}$) unique to the peer and send the third key to the insecure device and the peer (paragraphs 40-41).

Claim 36. A trusted media transaction system (210 of Fig. 2; Fig. 6) comprising

an insecure media player device (212 in Fig. 2; 614 in Fig. 6); and

a trusted secure token (214 in Fig. 2; 612 in Fig. 6) for performing an electronic transaction to obtain a first cryptographic key (K1; paragraph 59), accessing a message from the insecure device (N; paragraphs 61-62), creating a second cryptographic key (K2) from the message and the first key (712 in Fig. 7; paragraph 63), and allowing the insecure device to access the second key, the first key granting media file access rights (paragraphs 64-69), wherein the message is unique to the insecure device (paragraphs 64-69) and, in a file transaction with a

peer, the trusted secure token is configured to create a third key ($K_{2,2}$) unique to the peer and send the third key to the insecure device and the peer (paragraphs 40-41);

the insecure device configured to use the second key for media file decryption (paragraphs 64-69).

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-7, 9-24, 26-28 and 30-36 are rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent Application Publication No. 2003/0046568 to Riddick et al. ("Riddick").

(7) Arguments

The rejection of claims 1-7, 9-24, 26-28 and 30-36 under 35 U.S.C. §102(e) as being unpatentable over Riddick should be reversed.

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

- **Claims 1-7, 9-24, 26-28 and 30-36:**

Claims 1-7, 9-24, 26-28 and 30-36 are rejected under 35 U.S.C. §102(e) as being unpatentable over Riddick. The rejection should be reversed for at least the following reasons.

  - Independent Claim 1:

Independent claim 1 recites, "the secure token is configured to create a third key **unique to the peer** and **send the third key to the insecure device and the peer**." Riddick fails to teach at least these claimed features for at least the following reasons.

Riddick discloses a system and method for a consumer who owns a legitimate right to view an encrypted media item (14) to transfer the right to a friend (See paragraph [0082]). As Riddick discloses in Fig. 7 and paragraphs [0082]-[0087], in order to transfer the right to view the media item 14 from the consumer's smart token to his friend's smart token 18, the consumer inserts both his smart token and the friend's smart token into the player 52 and presses the SHARE button (see paragraph [0083] and step 82 in Fig. 7). In response, the player 52 retrieves the encrypted media key record from the consumer's smart token, decrypts it, decrements a count number, re-encrypts the media key record using public keys received from the friend's smart

token, and finally sends the new set of encrypted records to the friend's smart token (See paragraphs [0084]-[0086]). The friend's player can then use the new set of encrypted records to play the media item 14 (See paragraph 87, lines 1-4).

As such, in Riddick, the consumer's player 52 creates a new set of encrypted records using the public keys retrieved from the friend's smart token 18 and sends those new encrypted records back to the friend's smart token 18. However, the player 52 does not send the new set of encrypted records to the consumer's media player or insecure device. It appears that in Riddick, the player 52 would not send the new set of encrypted records to the consumer's insecure device because the consumer's smart token already has its own key or right to view the media item 14 to play the media item (See paragraphs [0082] and [0083]). Thus, there is no need for the player 52 to send the new set of encrypted records, which is unique to the friend's player, to the consumer's insecure device. Therefore, Riddick fails to teach "the secure token is configured to create a third key unique to the peer and **send the third key to the insecure device and the peer**," as recited in claim 1.

In the rejection of claim 1, the Examiner asserts that the "media key record" stored in the consumer's player of Riddick is the "third key" recited in claim 1 because the "[m]edia key record generated and stored on consumer secure token [is] read by consumer device and sent to peer's secure token," (See *Final Office Action*, page 4, lines 3-4). In addition, in the Response to Argument section, the Examiner argues that the media key record in Riddick is the claimed "third key" because "the media key ... is sent to the consumer device and later to the token of the peer whilst the consumer device generates the encrypted content," (See *Final Office Action*, last

line of page 2 and line 1 of page 3). However, those assertions are respectfully traversed. The "media key record" stored in the consumer's smart token is not sent to the friend. Rather, the key that is sent to the friend is a new set of encrypted records generated from the media key record and the public keys from the friend's smart token (See *Riddick*, paragraphs [0084]-[0086]). However, the "media key record" is not sent to the friend. As such, the "media key record" cannot be the "third key unique to the peer" as recited in claim 1. Furthermore, the new set of encrypted records that is sent to the friend cannot be the "third key" recited in claim 1, because the new set of encrypted records is not sent to the consumer's insecure device. Instead, the new set of encrypted records is sent to the smart token of the friend. As a result, again, Riddick fails to teach or suggest a secure token that creates a third key unique to the peer and sends the third key to both the insecure device and the peer, as recited in claim 1.

For at least the foregoing reasons, Riddick fails to teach each and every feature of independent claim 1 and thus cannot anticipate claim 1. It is therefore respectfully requested that the rejection of claim 1 be withdrawn, and claim 1 be allowed.

- Independent Claims 1, 11, 17, 19, 26, 28, and 36:

Independent claim 11 recites, "the processor is configured to create a third key unique to the peer and send the third key to the insecure device and the peer."

Independent claim 17 recites, "the smart card is configured to create a third key unique to the peer and send the third key to the insecure device and the peer."

Independent claim 19 recites, "in the file transaction, sending the third key to the insecure device and the peer."

Independent claim 28 recites, "the trusted secure device is configured to create a third key unique to the peer and send the third key to the insecure device and the peer."

Independent claim 36 recites, "the trusted secure token is configured to create a third key unique to the peer and send the third key to the insecure device and the peer."

As such, independent claims 1, 11, 17, 19, 28, and 36 recite features similar to those recited in independent claim 1 as discussed above. Thus, independent claims 1, 11, 17, 19, 28, and 36 are believed to be allowable over the cited documents of record for at least the same reasons as set forth above with respect to independent claim 1.

In addition, independent claim 26 recites an insecure device comprising, *inter alia*, "means for receiving a third cryptographic key derived from a message unique to a peer device, wherein the third cryptographic key is received by the peer device and used by the peer device for decryption." Thus, in claim 26, the insecure device receives the third cryptographic key that is also sent to the peer. As discussed with respect to claim 1 above, the player 52 in Riddick sends the new encrypted records to the friend's smart token but not to the consumer's player or insecure device. Accordingly, the insecure device in Riddick does not receive new encrypted records that are sent to the friend. Therefore, Riddick fails to teach or suggest an insecure device including "means for receiving a third cryptographic key derived from a message unique to a peer device," as recited in claim 26.

In view of the foregoing discussions, it is respectfully requested that the rejection of independent claims 11, 17, 19, 26, 28, and 36 be reversed and these claims be allowed.

- Claims 2-7, 9, 10, 12-16, 18, 20-24, 27, and 30-35:

Claims 2-7, 9, 10, 12-16, 18, 20-24, 27, and 30-35 are dependent from one of independent claims 1, 11, 17, 19, 26, 28, and 36. Therefore, they are believed to be allowable over the cited documents for at least the same reasons as set forth above. It is therefore respectfully requested that the rejection of dependent claims 2-7, 9, 10, 12-16, 18, 20-24, 27, and 30-35 be reversed and these claims be allowed.

(8) Conclusion

For at least the reasons given above, the rejection of claims 1-7, 9-24, 26-28 and 30-36 should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: December 21, 2009 By /Ashok K. Mannava/

Ashok K. Mannava
Registration No.: 45,301
(703) 652-3822

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. (Previously Presented) A secure token for use with an encrypted file and an insecure decryption device, the secure token comprising a processor for protecting a first cryptographic key against unauthorized access, and creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device, wherein, in a file transaction with a peer, the secure token is configured to create a third key unique to the peer and send the third key to the insecure device and the peer.

2. (Original) The secure token of claim 1 wherein the secure token includes a smart card, the smart card including the processor.

3. (Original) The secure token of claim 1, wherein the processor uses a hash function to create the second key from the message and the first key.

4. (Original) The secure token of claim 1, wherein the secure token performs an electronic transaction to obtain the first key.

5. (Original) The secure token of claim 4, wherein the secure token conducts a transaction with a server to purchase a desired file; and wherein the secure token receives the first key from the server.

6. (Previously Presented) The secure token of claim 4, wherein the transaction is a transaction of the secure token with the peer to purchase the file; and wherein the secure token receives the first key from the peer.

7. (Previously Presented) The secure token of claim 4, wherein the transaction is a transaction of the secure token with the peer to sell the file; and wherein the secure token sends the first key to the peer.

8. (Canceled)

9. (Original) The secure token of claim 1, further comprising means for receiving the first key and encrypted data, wherein the insecure device uses the second key to decrypt the encrypted data.

10. (Original) The secure token of claim 1, wherein processing power of the secure token is significantly less than processing power of the insecure device.

11. (Previously Presented) An article for a secure device, the secure device including a processor, the secure device used in combination with an insecure device, the article comprising memory encoded with data for instructing the processor to protect a first cryptographic key against unauthorized access, use a hash function to create a second cryptographic key from the

first key and a message unique to the insecure device, and send the second key to the insecure device, wherein, in a file transaction with a peer, the processor is configured to create a third key unique to the peer and send the third key to the insecure device and the peer.

12. (Original) The article of claim 11, wherein data further instructs the processor to perform an electronic transaction to obtain the first key.

13. (Original) The article of claim 12, wherein the secure device conducts a transaction with a server to purchase a desired file; and wherein the secure device receives the first key from the server.

14. (Previously Presented) The article of claim 13, wherein the transaction is a transaction of the secure device with the peer to purchase a file; and wherein the secure device receives the first key from the peer.

15. (Previously Presented) The article of claim 13, wherein the transaction is a transaction of the secure device with the peer to sell a file; and wherein the secure device sends the first key to the peer.

16. (Previously Presented) The article of claim 15, wherein the data further instructs the processor to create the third key.

17. (Previously Presented) A data rights management server for use with a media transaction system, the server comprising a processing unit programmed to cause the server to establish a secure channel with a smart card, access a unique identifier corresponding to an insecure device, send a first cryptographic key to the smart card via the secure channel, receive a unique identifier from the insecure device, create a second key from the first key and the identifier, encrypt a media file with the second key, and send the encrypted media file to the insecure device, the first key corresponding to the media file, wherein, in a transaction with a peer for the media file, the smart card is configured to create a third key unique to the peer and send the third key to the insecure device and the peer.

18. (Original) The server of claim 17, wherein the smart card and the server perform an electronic transaction for the first key.

19. (Previously Presented) A method of using an insecure decryption device for file distribution, the method comprising:

accessing a message unique to the insecure device;

accessing a first cryptographic key;

creating a second cryptographic key from the message and the first key;

allowing the insecure device to access the second key but not the first key; whereby the insecure device can use the second key for decryption;

in a file transaction with a peer, creating a third key that is unique to the peer; and

in the file transaction, sending the third key to the insecure device and the peer.

20. (Original) The method of claim 19, wherein a hash function is used to create the second key from the message and the first key.

21. (Original) The method of claim 19, wherein accessing the first key includes performing an electronic transaction to obtain the first key.

22. (Original) The method of claim 21, wherein the electronic transaction is conducted with a server to purchase a desired file; and accessing the first key includes receiving the first key from the server.

23. (Previously Presented) The method of claim 21, wherein the electronic transaction is conducted with the peer to purchase a file; and wherein accessing the first key includes receiving the first key from the peer.

24. (Previously Presented) The method of claim 21, wherein the electronic transaction is conducted with the peer to sell a file; the method further comprising sending the first key to the peer.

25. (Canceled)

26. (Previously Presented) An insecure device for use with a secure device and a first cryptographic key, the device comprising:

means for sending a message to the secure device, the message being unique to the insecure device;

means for receiving a second cryptographic key from the secure device, the second cryptographic key being derived from the message and the first cryptographic key;

means for performing decryption on a media file with the second cryptographic key;

means for receiving a third cryptographic key derived from a message unique to a peer device, wherein the third cryptographic key is received by the peer device and used by the peer device for decryption; and

means for encrypting the decrypted media file with the third cryptographic key.

27. (Original) The device of claim 26, further comprising means for playing media decrypted with the second cryptographic key.

28. (Previously Presented) A trusted system for file distribution, the system comprising:

an insecure device; and

a trusted secure device for storing a first cryptographic key, accessing a message from the insecure device wherein the message is unique to the insecure device, creating a second

cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting file access rights;

the insecure device not allowed to access the first key, the insecure device using the second key for decryption, wherein, in a file transaction with a peer, the trusted secure device is configured to create a third key unique to the peer and send the third key to the insecure device and the peer.

29. (Canceled).

30. (Original) The system of claim 28, wherein the secure device is a secure token.

31. (Original) The system of claim 30, wherein the secure token includes a smart card.

32. (Original) The system of claim 31, wherein the insecure device includes a media player.

33. (Original) The system of claim 28, wherein the secure device is configured to perform an electronic transaction to obtain the first key.

34. (Original) The system of claim 28, wherein processing power of the secure device is significantly less than processing power of the insecure device.

35. (Original) The system of claim 28, further comprising a peer-to-peer application for identifying peers having desired files.

36. (Previously Presented) A trusted media transaction system comprising

an insecure media player device; and

a trusted secure token for performing an electronic transaction to obtain a first cryptographic key, accessing a message from the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting media file access rights, wherein the message is unique to the insecure device and, in a file transaction with a peer, the trusted secure token is configured to create a third key unique to the peer and send the third key to the insecure device and the peer;

the insecure device configured to use the second key for media file decryption.

(10) Evidence Appendix

None.

(11) Related Proceedings Appendix

None.